INFORMATION ASSURANCE & CONNECTION POLICY

Mandatory IAW USFK Reg 350-2, CJCSM 6510.01 and DODD 8570.1

<u>IA Overview</u>:

IA Defined

The Threat

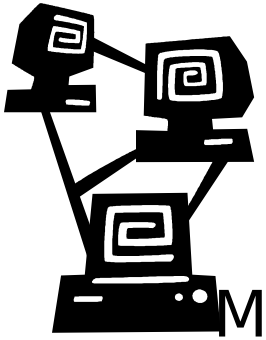
The Impact

Your Responsibilities

What is IA?

INFORMATION ASSURANCE

IA functions to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.



Measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities

The Threat

- Information and information systems are always vulnerable. Never let your guard down.

- Greatest threat – the user… YOU!
  - What you don’t know
  - What you do wrong

- Other threats
  - Malicious logic (worms/viruses/trojans)
  - Hackers

The Impact

- Your computer or network could be used by someone to damage our

Command and Control.

- Someone could get access to our informatic

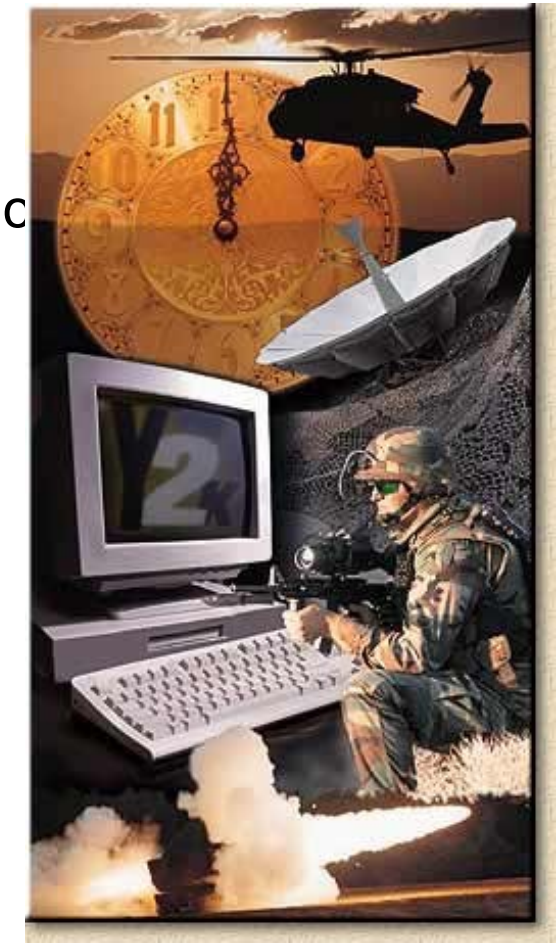
including YOUR personal information.

- Computers and network functions

(i.e.: e-mail) could be lost, or the network could go down.

- Commanders and all personnel might be

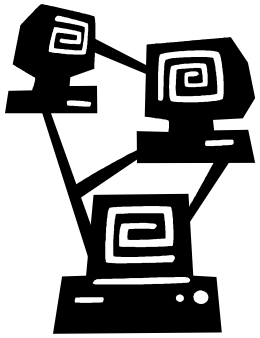
unable to do our jobs. People could die.



What is required?

CONNECTION POLICY

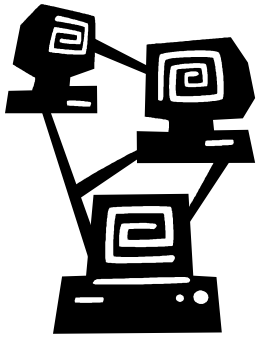
CFC/USFK networks have experienced real-world compromises due to improper preparation of information systems or enclaves that were connected.



USFK has set a goal to ensure the availability of information and information systems throughout the Korean Theater of Operations (KTO) by preventing the spread of computer and network vulnerabilities.

Security Baseline

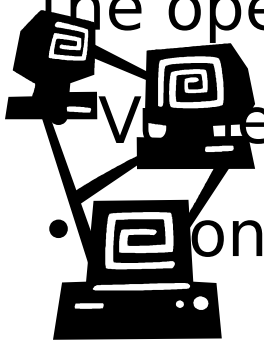
Prior to connecting any system to the CFC/USFK networks; a security baseline package must be submitted to the appropriate USFK Designated Approving Authority (DAA) for connection approval.



If deploying to Korea, your originating/home DAA needs to provide a signed statement verifying the items in the security baseline have been accomplished.

Verification Items Required

- DoD IAVA compliance patching and verification
- Anti-virus signature file update and system virus scanning
- Latest application service packs and updates for the operating system
- Vulnerability assessment/scanning
- Strong complexity for all passwords



Your originating/home DAA needs to provide a signed statement verifying the items above have been accomplished.

Let's Review!

Your Critical IA Responsibilities

- Receive your initial and annual training

Training can be in the form of classroom training, video presentations, personalized instruction, Computer-Based Training (CBT), Web-Based Training (WBT), read-and-sign briefings, or any combination of those methods.

- Protect your passwords (memorize them!)

If written down, they must be stored in a safe

- ***Never*** give out your userID and password

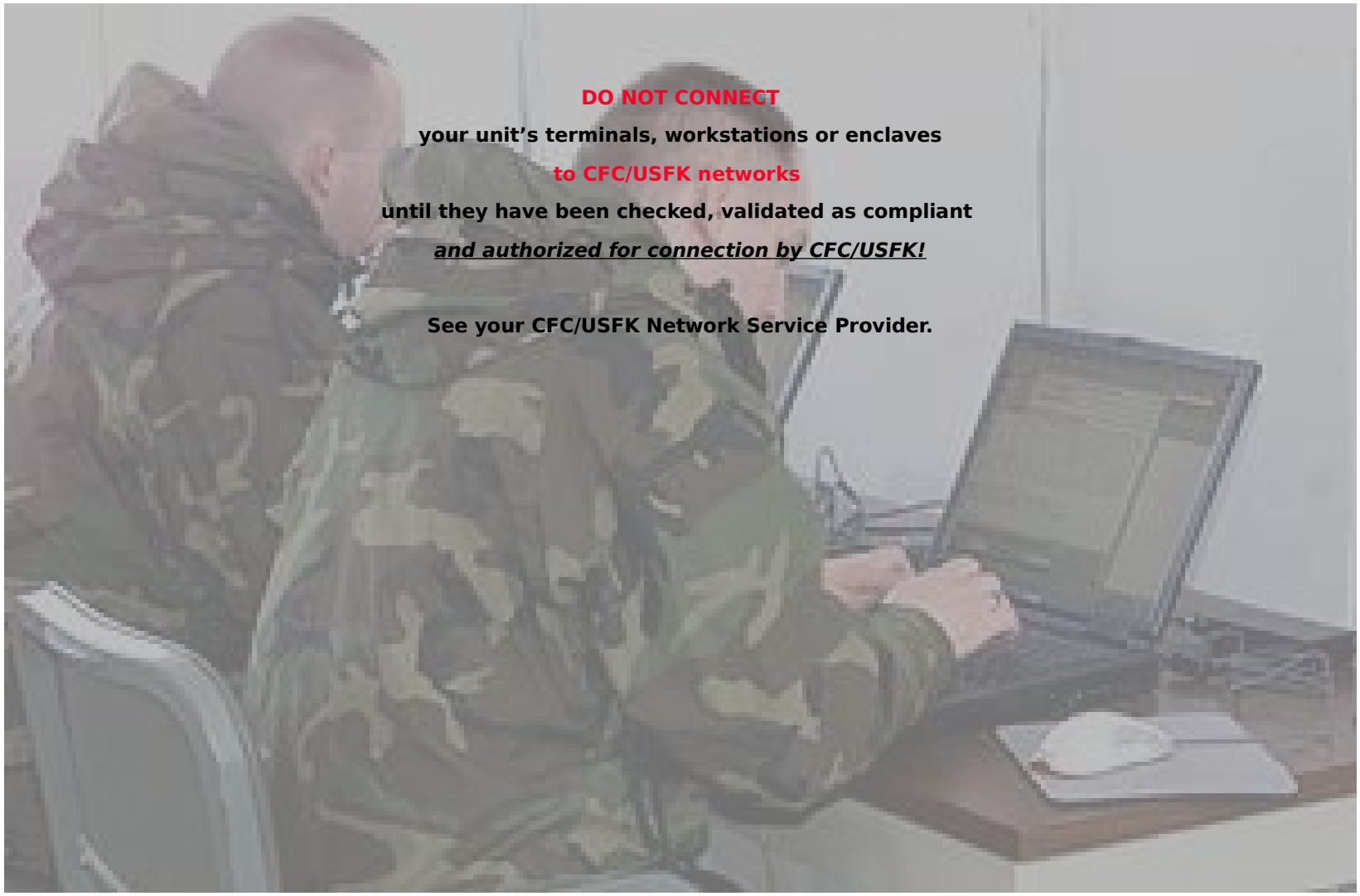
Your Critical IA Responsibilities

- Never leave your workstation unattended *and* unlocked
- Government computers are for official use only
- Don't download unofficial email attachments
- Don't download files or software from unofficial websites
- Make sure your workstation's antivirus software is updated

Your Critical IA Responsibilities

- Scan removable media (including thumb drives) with antivirus software
- Report strange or suspicious activities!
- *Never* connect a classified system to an unclassified or lower-classified network
- Above all…

Your Critical IA Responsibilities



DO NOT CONNECT

your unit's terminals, workstations or enclaves

to CFC/USFK networks

until they have been checked, validated as compliant

and authorized for connection by CFC/USFK!

See your CFC/USFK Network Service Provider.

Summary

Information and systems are always vulnerable.
Never let your guard down!

The greatest threat is **us**.
Carry out your IA Responsibilities!

CFC/USFK IA-CJ62
DSN 725-8213
j6iamail@korea.army.mil